**Investigation**

**Reoccurring issue identified:**

Weak access controls and misconfigured databases, and SQL injection.

Databases are the backbone of most modern web applications, and often times they contain sensitive or even confidential information. There are a number of well know, major data breaches that have occurred due to misconfigured or unsecured databases.

**Examples:**

1. **Equifax (2017)**: Personal data of 147 million people compromised due to a vulnerability in Apache Struts, which allowed attackers to access a database containing sensitive information.
   1. **Source -** [**https://archive.epic.org/privacy/data-breach/equifax/**](https://archive.epic.org/privacy/data-breach/equifax/)
2. **Marriott International (2018)**: Information of up to 500 million guests compromised due to unauthorized access to the Starwood guest reservation database.
   1. **Source** - [https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen](https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html#:~:text=In%20late%202018%2C%20the%20Marriott,being%20exfiltrated%20by%20the%20attackers.)
3. **Yahoo (2013-2014)**: Over 3 billion accounts compromised due to unauthorized access to Yahoo’s user database.
   1. **Source** - <https://en.wikipedia.org/wiki/Yahoo!_data_breaches>
4. **eBay (2014)**: Personal information of 145 million users exposed due to unauthorized access to a database containing user records.
   1. **Source** - <https://www.twingate.com/blog/tips/ebay-data-breach>
5. **Target (2013)**: Payment card information of 40 million customers stolen due to unauthorized access to a database through compromised vendor credentials.
   1. **Source** - [https://www.commerce.senate.gov](https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883)

1. **LinkedIn (2012)**: Over 160 million accounts affected due to unauthorized access to a database containing hashed passwords.
   1. **Source** - <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/2012-linkedin-breach-117-million-emails-and-passwords-stolen-not-6-5m>
2. **Adobe (2013)**: Information of 38 million active users exposed due to unauthorized access to a database containing user information and passwords.
   1. **Source** - <https://www.linkedin.com/pulse/adobe-cyberattack-2013-case-study-bulitha-kawushika-hlrxc/>

1. **Uber (2016)**: Personal data of 57 million users and drivers exposed due to unauthorized access to a database stored in a GitHub repository.
   1. **Source** - <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/uber-breach-exposes-the-data-of-57-million-drivers-and-users>
2. **Anthem Inc. (2015)**: Personal information of 78.8 million individuals exposed due to unauthorized access to a database containing customer data.
   1. **Source** - <https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm>

**Reference Scenario:**

Azumer water, a FEMA org that provides water during disasters, fell victim to an attack on their database systems via a social engineering attack. I performed a security assessment on their systems and identified the following critical vulnerabilities that need addressed ASAP**.**

**Critical Vulnerabilites:**

Database access is unrestricted

Database users have excess permissions

Volunteer Database contains PII that should be separated into another database with more strict permissions.

~~SQL injection vulnerabilities are present in the azumer-water.org website~~

~~Database web portal allows unauthenticated access~~

Weak passwords are in use

**Planning & Implementtation**

**Parametrize the web application to prevent SQL injection. – DONE**

**2. Implement a login portal to prevent unauthorized access to the azumer-water.org database page – STEPS Taken to remediate**

**Created a database for authenticating users on the web portal named azumer\_web\_auth**

**Created a table called users with the fields id and password**

**A screen shot of a computer

Description automatically generated**

**Added a single user for the webserver, the password is stored in a sha256 hash**

**A screen shot of a computer program

Description automatically generated**

**New Landing Login Page**

**A screenshot of a computer

Description automatically generated**

**Page after successful login**

**A screenshot of a computer

Description automatically generated**

**Page After failed Login**

**A screenshot of a login screen

Description automatically generated**

**END 2.**